

日本国特許庁
JAPAN PATENT OFFICE

M. Shimamoto
3/19/04
Q 80572
1 of 1

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 3月28日

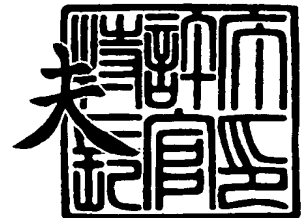
出願番号
Application Number: 特願2003-091782
[ST. 10/C]: [JP 2003-091782]

出願人
Applicant(s): NECマイクロシステム株式会社

2004年 1月16日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



出証番号 出証特2003-3112280

【書類名】 特許願

【整理番号】 01220096

【提出日】 平成15年 3月28日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 1/00

【発明者】

【住所又は居所】 神奈川県川崎市中原区小杉町 1 丁目 4 0 3 番 5 3 エヌ
イーシーマイクロシステム株式会社内

【氏名】 島本 光裕

【特許出願人】

【識別番号】 000232036

【氏名又は名称】 エヌイーシーマイクロシステム株式会社

【代理人】

【識別番号】 100088328

【弁理士】

【氏名又は名称】 金田 暢之

【電話番号】 03-3585-1882

【選任した代理人】

【識別番号】 100106297

【弁理士】

【氏名又は名称】 伊藤 克博

【選任した代理人】

【識別番号】 100106138

【弁理士】

【氏名又は名称】 石橋 政幸

【手数料の表示】

【予納台帳番号】 089681

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9712889

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 半導体集積回路装置

【特許請求の範囲】

【請求項 1】 内部クロックに同期して動作する複数の内部回路を備えた半導体集積回路装置であって、

所定周期の第 1 のクロックを生成するクロック生成回路と、

前記第 1 のクロックから一部のパルスの間引いた間欠するパルス列である第 2 のクロックを生成し、前記内部クロックとして前記内部回路にそれぞれ供給する間欠クロック生成回路と、

第 1 のクロックから間引かれるパルス列である第 3 のクロックのタイミングで電源電流を消費する電流発生回路と、
を有する半導体集積回路装置。

【請求項 2】 前記間欠クロック生成回路は、

時間軸上で出力データが変化する変動データ出力回路と、

前記変動データ出力回路の出力データにしたがって前記第 3 のクロックを生成するタイミング生成回路と、

前記第 3 のクロックと前記クロック生成回路から出力される第 1 のクロックとを入力とし、前記第 3 のクロックのタイミングで前記第 1 のクロックの出力を停止することで前記第 2 のクロックを生成する同期回路と、
を有する請求項 1 記載の半導体集積回路装置。

【請求項 3】 複数の前記電流発生回路から成る電流発生回路群と、

予め設定された値にしたがって、前記電源電流を消費させる前記電流発生回路を選択する回路選択レジスタと、
を有する請求項 1 または 2 記載の半導体集積回路装置。

【請求項 4】 複数の前記電流発生回路から成る電流発生回路群と、

前記変動データ出力回路の出力データにしたがって、前記電源電流を消費させる前記電流発生回路を選択する回路選択レジスタと、
を有する請求項 1 または 2 記載の半導体集積回路装置。

【請求項 5】 前記変動データ出力回路は、

乱数を生成する乱数発生回路である請求項 1 乃至 4 のいずれか 1 項記載の半導体集積回路装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、内部クロックに同期して動作する複数の内部回路を備えたマイクロコンピュータ等の半導体集積回路装置に関する。

【0002】

【従来の技術】

近年、マイクロコンピュータ等の半導体集積回路装置の多くは、高集積化、低消費電流化に有利な CMOS によって各種内部回路が構成されている。この CMOS 回路は、出力状態が“1”から“0”あるいは“0”から“1”に変化するときに電源電流を消費する。特に、大きな容量性負荷が接続されるバスラインを半導体集積回路装置内に備えている場合は、バスライン上を流れるデータが“1”から“0”あるいは“0”から“1”に変化するときに大きな電流が消費される。このことは、半導体集積回路装置の消費電流を観測することで半導体集積回路装置の内部で実行されているデータ処理の手順や処理されているデータが読み取られる可能性があることを意味する。すなわち、半導体集積回路装置の消費電流を観測することで、どのようなデータがバスライン上を流れているかが分かり、さらには半導体集積回路装置がどのように動作しているのか、どのようなデータが処理されているのかが読み取られてしまうおそれがある。そこで、消費電流波形の観測によるデータの再生を実質的に不可能にして、半導体集積回路装置内に保存されたユーザーのプログラムやデータを保護することが必要になる。

【0003】

従来は、プログラムやデータを保護する方法として、プログラムやデータ自体を暗号化する手法が提案され、例えば特許文献 1 に、暗号化に用いる乱数を生成するための擬似乱数発生回路が記載されている。

【0004】

【特許文献 1】

特許第 2,937,919 号

【0005】

【発明が解決しようとする課題】

上記消費電流波形のデータ依存性を低減する簡易な手法としては、例えば、データの変化に依存しない所定周期の偽電流を常時半導体集積回路装置内に流す手法が考えられる。

【0006】

しかしながら、偽電流を常時流す手法では半導体集積回路装置の消費電流が増大するため、該半導体集積回路装置を利用できる用途が限定されてしまう問題がある。また、消費電流波形を観測することで偽電流の存在が判別されるおそれもあるため、プログラムやデータの保護性能が低いという問題もある。

【0007】

本発明は上記したような従来技術が有する問題点を解決するためになされたものであり、消費電流を不必要に増大させることなく、消費電流波形を観測することによるデータの再生を困難にして、データ処理の手順や処理されるデータの保護性能を向上させた半導体集積回路装置を提供することを目的とする。

【0008】

【課題を解決するための手段】

上記目的を達成するため本発明の半導体集積回路装置は、内部クロックに同期して動作する複数の内部回路を備えた半導体集積回路装置であって、

所定周期の第1のクロックを生成するクロック生成回路と、

前記第1のクロックから一部のパルスの間引いた間欠するパルス列である第2のクロックを生成し、前記内部クロックとして前記内部回路にそれぞれ供給する間欠クロック生成回路と、

第1のクロックから間引かれるパルス列である第3のクロックのタイミングで電源電流を消費する電流発生回路と、
を有する構成である。

【0009】

このとき、前記間欠クロック生成回路は、

時間軸上で出力データが変化する変動データ出力回路と、

前記変動データ出力回路の出力データにしたがって前記第3のクロックを生成するタイミング生成回路と、

前記第3のクロックと前記クロック生成回路から出力される第1のクロックとを入力とし、前記第3のクロックのタイミングで前記第1のクロックの出力を停止することで前記第2のクロックを生成する同期回路と、
を有する構成であってもよい。

【0010】

また、複数の前記電流発生回路から成る電流発生回路群と、

予め設定された値にしたがって、前記電源電流を消費させる前記電流発生回路を選択する回路選択レジスタと、
を有していてもよく、

複数の前記電流発生回路から成る電流発生回路群と、

前記変動データ出力回路の出力データにしたがって、前記電源電流を消費させる前記電流発生回路を選択する回路選択レジスタと、
を有していてもよい。

【0011】

また、前記変動データ出力回路は、

乱数を生成する乱数発生回路であってもよい。

【0012】

上記のように構成された半導体集積回路装置では、第1のクロックから一部のパルスを間引いた間欠するパルス列である第2のクロックを生成し、内部クロックとして内部回路にそれぞれ供給する間欠クロック生成回路と、第1のクロックから間引かれるパルス列である第3のクロックのタイミングで電源電流を消費する電流発生回路とを有することで、内部回路が間欠するパルス列である第2のクロックで動作していても、消費電流波形は内部回路が第1のクロックで動作している通常動作時と同様に変動する。

【0013】

【発明の実施の形態】

次に本発明について図面を参照して説明する。

【0014】

(第1の実施の形態)

図1は本発明の半導体集積回路装置の第1の実施の形態の構成を示す回路図であり、図2は図1に示した半導体集積回路装置の動作を示すタイミングチャートである。

【0015】

図1に示すように、本実施形態の半導体集積回路装置は、中央処理装置(CPU)103と、記憶装置であるROM104、RAM105、及びEEPROM106と、半導体集積回路装置の外部とデータを送受信するためのインタフェースである入出力ポート(I/O)107と、所定周期のクロックA(第1のクロック)を生成するクロック生成回路101と、クロックAから一部のパルスの間引いた間欠するパルス列であるクロックC(第2のクロック)を生成する間欠クロック生成回路100と、クロックAから間引かれるパルス列であるクロックB(第3のクロック)のタイミングで電源電流を消費する電流発生回路102とを有する構成である。

【0016】

間欠クロック生成回路100は、乱数を生成する乱数発生回路108と、乱数発生回路108から出力された乱数を一時的に保持するレジスタ109と、乱数発生回路108から出力される乱数にしたがって上記クロックBを生成するタイミング生成回路110と、クロックB及びクロックAを入力とし、クロックBのタイミングでクロックAの出力を停止することでクロックCを生成する同期回路111とを有する構成である。

【0017】

なお、図1では半導体集積回路装置の内部回路として、CPU103、ROM104、RAM105、EEPROM106、及びI/O107を備えた構成を示しているが、内部回路はこれらに限定されるものではなく、半導体集積回路装置は、他の機能を有する不図示の様々な回路を備えている。

【0018】

第1の実施の形態の半導体集積回路装置は、内部回路を動作させる内部クロックとして、クロックAから一部のパルスの間引いた間欠するパルス列であるクロックCを用いる構成であり、さらにクロックAから間引かれるパルス列であるクロックBのタイミングで電流発生回路102を動作させる構成である。

【0019】

クロック生成回路101は、所定周期のクロックAを生成して同期回路111に供給する。このクロックAは、間欠するパルス列であるクロックCを用いない場合に、CPU103、ROM104、RAM105、EEPROM106、I/O107、及び乱数発生回路108等の半導体集積回路装置の各種内部回路を同期して動作させるための内部クロックとして使用される。

【0020】

なお、クロック生成回路101は、周知の水晶発振器やリングオシレータ等を用いて内部クロックを発振する回路であってもよく、外部から供給されるクロックから内部クロックを生成する回路であってもよい。また、外部から供給される信号にしたがって、例えば発振出力や発振停止が制御される構成であってもよい。

【0021】

タイミング生成回路110は、乱数発生回路108で生成された乱数をレジスタ109を介して受け取り、例えば、乱数の値が予め任意に設定された値と一致するときに“1”となるクロックBを生成する。

【0022】

同期回路111は、クロックBとクロック生成回路101から出力されるクロックAとを入力とし、クロックBが“1”のときに出力を停止させて間欠するパルス列であるクロックCを生成する。このクロックCを用いて半導体集積回路装置の内部回路（上記CPU103、記憶装置、I/O107等）を動作させる。さらに、本実施形態では、電流発生回路102をクロックAから間引かれるパルス列であるクロックBのタイミングで動作させる。このように動作させることで、内部回路が間欠するパルス列であるクロックCで動作していても、消費電流波形は内部回路がクロックAで動作している通常動作時と同様に変動する。したが

って、消費電流波形を観測しても通常動作時と区別することが困難であり、かつ消費電流波形からデータとの依存性を解析することが困難になる。

【0023】

なお、乱数発生回路108には、例えば、周知のリニアフィードバックシフトレジスタ (Linear Feedback Shift Register) を利用した、擬似乱数を発生する擬似乱数発生回路等を用いればよい。

【0024】

また、電流発生回路102は、例えば、図3に示すように、電源VDDと接地電位GND間に挿入される、直列に接続された抵抗器R及びnチャネルMOSトランジスタQ1を用いて構成すればよい。この場合、電流発生回路102に流れる電流値は抵抗器Rの値によって決定される。

【0025】

次に、本実施形態の半導体集積回路装置の動作について図2を用いて説明する。なお、図2に示すタイミングチャートは、クロックAにより半導体集積回路装置の内部回路を動作させる通常動作の場合と、電流発生回路102をもたずにクロックCにより半導体集積回路装置の内部回路を間欠して動作させる場合と、クロックCにより半導体集積回路装置の内部回路を動作させ、かつ電流発生回路102をクロックBにより動作させる場合との消費電流波形をそれぞれ示している。

【0026】

図2に示すように、クロックAにより半導体集積回路装置の内部回路を動作させる通常動作の場合に比べて、電流発生回路102をもたずにクロックCにより半導体集積回路装置の内部回路を間欠的に動作させると、消費電流は低減するが、通常とは明らかに異なる動作をしていることが外部から判別されてしまう。そのため、半導体集積回路装置の内部処理動作を外部から解析し難くするという効果が低減してしまう。

【0027】

一方、本実施形態のように、クロックCにより半導体集積回路装置の内部回路を動作させると同時に電流発生回路102をクロックBで動作させると、消費電

流はクロック A により半導体集積回路装置の内部回路を動作させる通常動作時と同程度になるが、消費電流波形が通常動作の場合と判別し難くなるため、消費電流波形を観測することでデータとの依存性を解析して再生することが困難になることが分かる。

【0028】

したがって、本実施形態の半導体集積回路装置によれば、半導体集積回路装置の内部回路を間欠的に動作させると同時に電流発生回路を間欠的に動作させることで、消費電流波形が通常の場合と判別し難くなるため、消費電流波形のデータとの依存性の解析が困難になり、データの処理手順や処理されるデータの保護能力を高めることができる。また、偽電流を常時流す必要も無いため、消費電流を不必要に増大させることがない。

【0029】

(第2の実施の形態)

図4は本発明の半導体集積回路装置の第2の実施の形態の構成を示す回路図である。

【0030】

図4に示すように、第2の実施の形態の半導体集積回路装置は、複数の電流発生回路 $102_1 \sim 102_n$ (n は正の整数) から成る電流発生回路群 113 と、動作させる電流発生回路を選択するための回路選択レジスタ 112 とを図1に示した第1の実施の形態の半導体集積回路装置に追加した構成である。その他の構成及び動作は第1の実施の形態と同様であるため、その説明は省略する。

【0031】

回路選択レジスタ 112 は、例えばデータバスを介して任意の値が書き込み可能に設けられ、複数の電流発生回路 $102_1 \sim 102_n$ は、予め回路選択レジスタ 112 に書き込まれた値にしたがって選択され、タイミング生成回路から出力されるクロック B によって動作する。

【0032】

例えば、回路選択レジスタ 112 のビット 0 を電流発生回路 113_1 に割り当てた場合、回路選択レジスタ 112 の値が “1H”、すなわちビット 0 が “1”

のときに電流発生回路 113_1 がクロック B により動作する。同様に、回路選択レジスタ 112 の他のビットに割り当てられた電流発生回路 $102_2 \sim 102_n$ は、対応するビットが“1”のときにクロック B により動作する。なお、電流発生回路 $102_1 \sim 102_n$ は、1つだけ選択されて動作してもよく、複数が選択されて同時に動作してもよい。

【0033】

本実施形態の半導体集積回路装置によれば、第1の実施の形態の半導体集積回路装置の効果に加えて、複数の電流発生回路 $102_1 \sim 102_n$ から選択された回路を動作させることで、消費電流波形をより通常の動作に近い形にすることができるため、消費電流波形を観測することによるデータとの依存性の解析をより困難にすることができる。

【0034】

(第3の実施の形態)

図5は本発明の半導体集積回路装置の第3の実施の形態の構成を示す回路図である。

【0035】

図5に示すように、第3の実施の形態の半導体集積回路装置は、乱数発生回路で生成された乱数が、該乱数を一時的に保持するためのレジスタ 209 を介して回路選択レジスタ 212 に供給される構成である。その他の構成及び動作は第2の実施の形態と同様であるため、その説明は省略する。

【0036】

本実施形態の半導体集積回路装置は、乱数を一時的に保持するレジスタ 209 の値を回路選択レジスタ 212 でも取り込むことによりクロック B で動作する電流発生回路がランダムに選択される。

【0037】

本実施形態の半導体集積回路装置によれば、複数の電流発生回路からランダムに選択された回路をクロック B で動作させるため、第2の実施の形態の半導体集積回路装置よりも消費電流波形を観測することによるデータとの依存性の解析をさらに困難にすることができる。

【0038】

なお、上述した第1の実施の形態～第3の実施の形態では、乱数発生回路から出力される乱数を用いてタイミング生成回路や電流発生回路を動作させる例を示したが、乱数に代えて、半導体集積回路装置が備えるタイマやシフトレジスタあるいは内部バス等のように半導体集積回路装置の動作中に時間軸上で出力データが変化する回路（変動データ出力回路）の出力値を用いることも可能である。

【0039】

【発明の効果】

本発明は以上説明したように構成されているので、以下に記載する効果を奏する。

【0040】

第1のクロックから一部のパルスの間引いた間欠するパルス列である第2のクロックを生成し、内部クロックとして内部回路にそれぞれ供給する間欠クロック生成回路と、第1のクロックから間引かれるパルス列である第3のクロックのタイミングで電源電流を消費する電流発生回路とを有することで、内部回路が間欠するパルス列である第2のクロックで動作していても、消費電流波形は内部回路が第1のクロックで動作している通常動作時と同様に変動する。

【0041】

したがって、消費電流波形を観測しても通常動作時と区別することが困難であり、かつ消費電流波形を観測することでデータとの依存性を解析し、データの処理手順や処理されるデータを再生することが困難となる。よって、データの処理手順や処理されるデータの保護能力を向上させることができる。また、偽電流を常時流す必要も無いため、消費電流を不必要に増大させることがない。

【図面の簡単な説明】

【図1】

本発明の半導体集積回路装置の第1の実施の形態の構成を示す回路図である。

【図2】

図1に示した半導体集積回路装置の動作を示すタイミングチャートである。

【図3】

図1に示した電流発生回路の一構成例を示す回路図である。

【図4】

本発明の半導体集積回路装置の第2の実施の形態の構成を示す回路図である。

【図5】

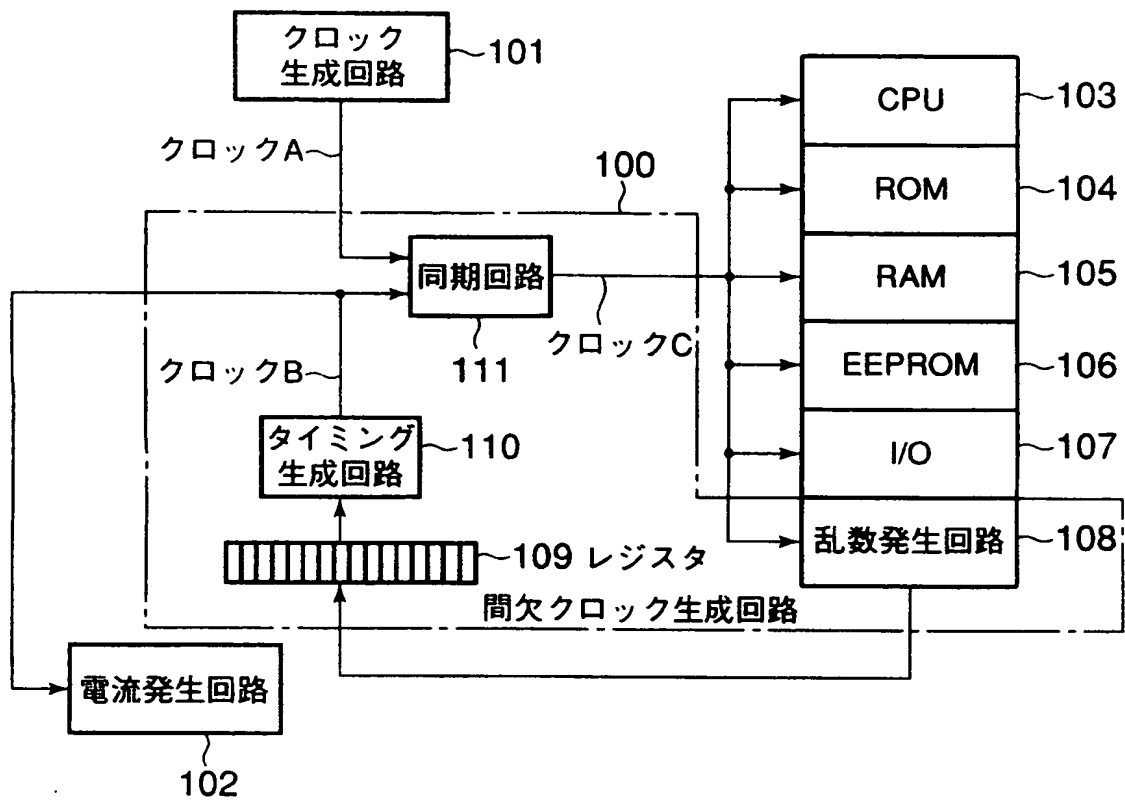
本発明の半導体集積回路装置の第3の実施の形態の構成を示す回路図である。

【符号の説明】

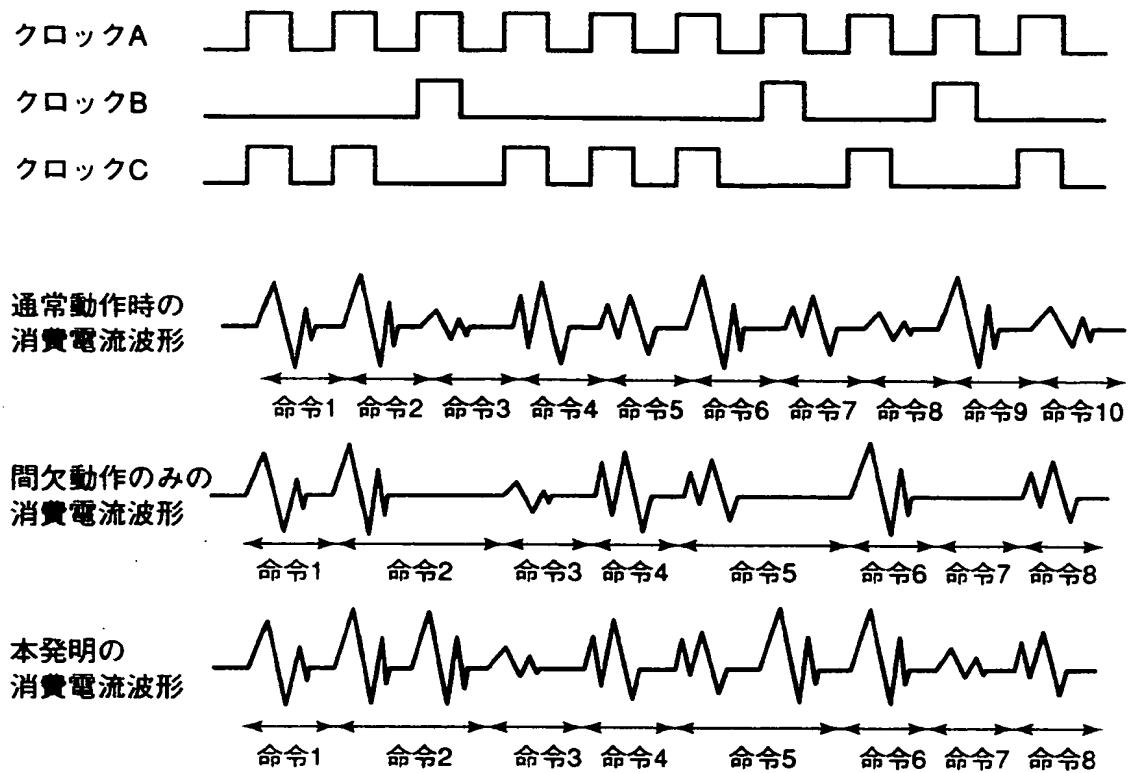
- 100 間欠クロック生成回路
- 101 クロック生成回路
- 102、102₁～102_n 電流発生回路
- 103 CPU
- 104 ROM
- 105 RAM
- 106 EEPROM
- 107 I/O
- 108 乱数発生回路
- 109、209 レジスタ
- 110 タイミング生成回路
- 111 同期回路
- 112、212 回路選択レジスタ
- 113 電流発生回路群
- Q1 nチャネルMOSトランジスタ
- R 抵抗器

【書類名】 図面

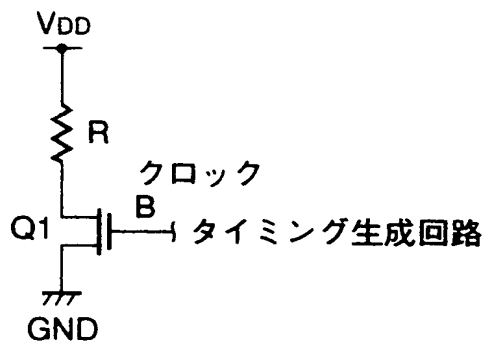
【図 1】



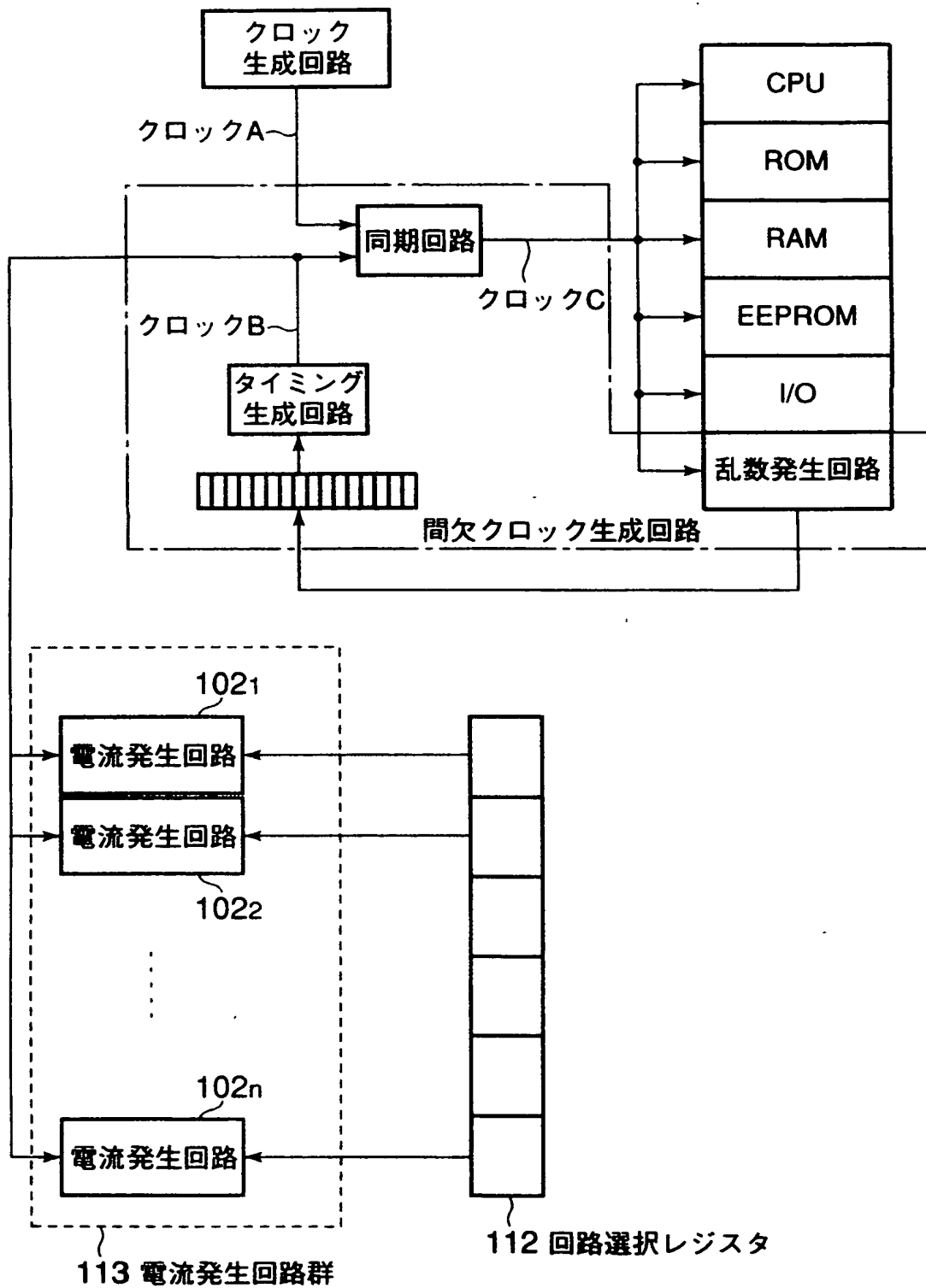
【図2】



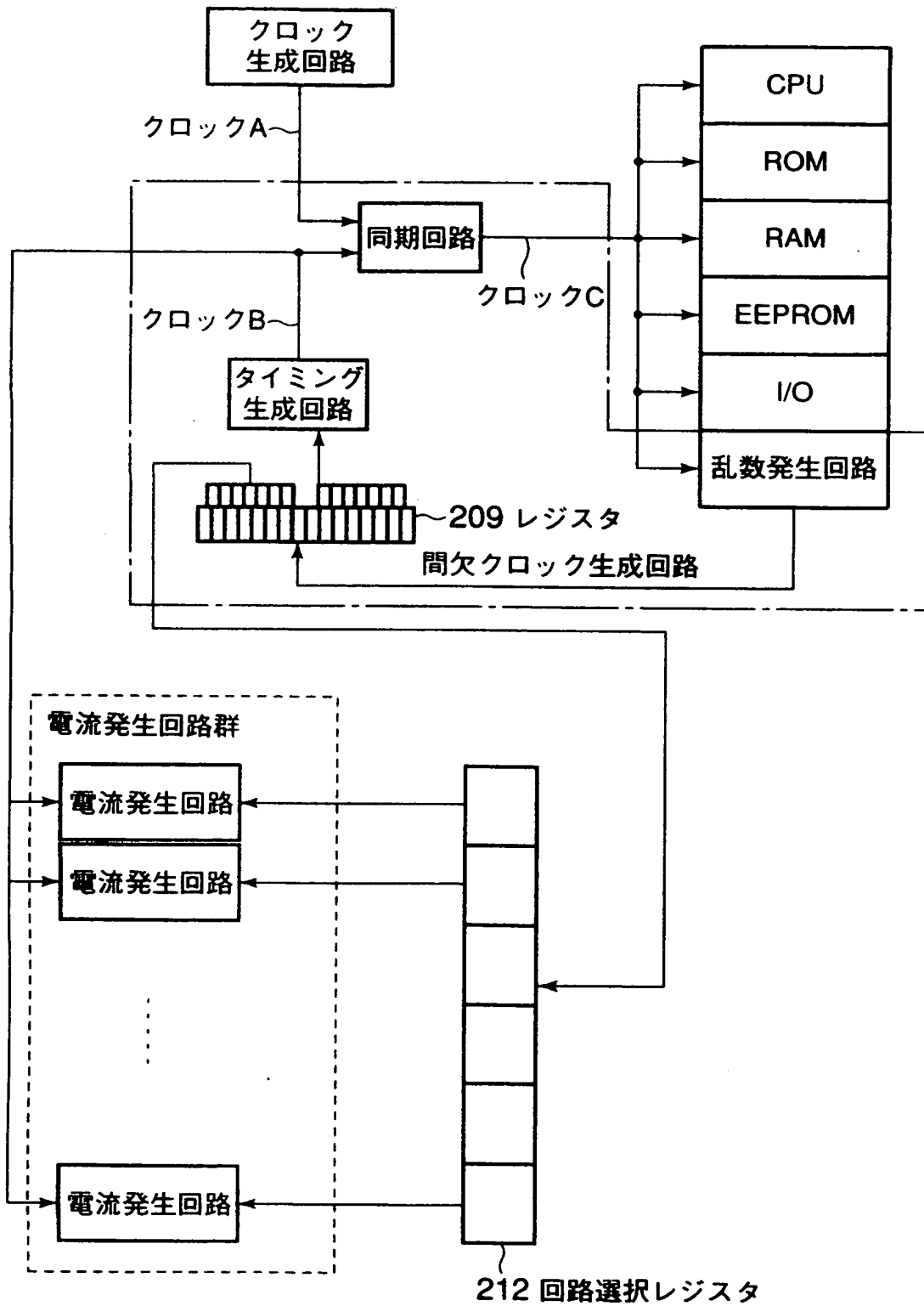
【図3】



【図4】



【図5】



【書類名】 要約書

【要約】

【課題】 消費電流を不必要に増大させることなく、消費電流波形を観測することによるデータの再生を困難にして、データ処理の手順や処理されるデータの保護性能を向上させた半導体集積回路装置を提供する。

【解決手段】 内部クロックに同期して動作する複数の内部回路を備えた半導体集積回路装置であって、所定周期の第1のクロックを生成するクロック生成回路と、第1のクロックから一部のパルスの間引いた間欠するパルス列である第2のクロックを生成し、内部クロックとして内部回路にそれぞれ供給する間欠クロック生成回路と、第1のクロックから間引かれるパルス列である第3のクロックのタイミングで電源電流を消費する電流発生回路とを有する構成とする。

【選択図】 図1

特願 2 0 0 3 - 0 9 1 7 8 2

出 願 人 履 歴 情 報

識別番号 [0 0 0 2 3 2 0 3 6]

1. 変更年月日 2 0 0 1 年 5 月 2 1 日
[変更理由] 名称変更
住 所 神奈川県川崎市中原区小杉町1丁目403番53
氏 名 エヌイーシーマイクロシステム株式会社
2. 変更年月日 2 0 0 3 年 7 月 3 0 日
[変更理由] 名称変更
住 所 神奈川県川崎市中原区小杉町1丁目403番53
氏 名 N E C マイクロシステム株式会社